

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

ECOLAB Inc., and NALCO COMPANY,
LLC d/b/a Nalco Water, an Ecolab Company
and/or Nalco Water,

Plaintiffs,

v.

JESSICA GRAILER,

Defendant.

No. 3:23-cv-00102

**MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' MOTION FOR
TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION**

Pursuant to Rule 65(a) and (b) of the Federal Rules of Civil Procedure, Plaintiffs Ecolab, Inc. ("Ecolab") and Nalco Company LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water ("Nalco") (hereafter Ecolab and Nalco may be collectively referred to as "Company," "Nalco/Ecolab," or "Plaintiffs") state as follows in support of its Motion for a Temporary Restraining Order and Preliminary Injunction.

I. PRELIMINARY STATEMENT

Nalco/Ecolab brings this lawsuit against their former Account Manager who shortly before and even after voluntarily resigning from the Company to join a competitor, accessed Plaintiffs' computer network and misappropriated hundreds of files containing Plaintiffs' confidential and trade secret information. Plaintiffs seek damages and preliminary injunctive relief enjoining Defendant from further misappropriating Plaintiffs' highly confidential and trade secret information and requiring her to preserve and return to Plaintiff its data. Plaintiffs' attempt to get Defendant to voluntarily preserve and return Plaintiffs' information was ignored.

Plaintiffs are asserting claims against Defendant Grailer for: violations of the federal Defend Trade Secrets Act; violations of the Wisconsin Uniform Trade Secrets Act, violations of the federal Computer Fraud and Abuse Act, Defendant's breach of her Ecolab Employee Agreement, breach of the covenant of good faith and fair dealing, and unjust enrichment.

II. BACKGROUND

A. Nalco/Ecolab

Nalco/Ecolab are a leading developer and provider of water, hygiene, and infection prevention solutions and services geared toward protecting people and vital resources. Ecolab provides a broad spectrum of products and services to businesses throughout the United States including the State of Wisconsin. They partner with companies across a wide range of industries to develop solutions for its customers specific water needs.

B. Defendant Grailer's Employment with Nalco/Ecolab

Grailer is a former Account Manager for the Company in its Northwest region and was based in Verona, Wisconsin. *See Exhibit A*, Gallart Declaration at ¶ 5. As an Account Manager, Defendant Grailer managed accounts in the States of Wisconsin, Minnesota, and Illinois. *See id.* Grailer's job responsibilities included managing client water treatment processes, such as reviewing and analyzing technical chemical treatment data, reviewing operations and procedures, managing and troubleshooting chemical formulations and reformulations, maintaining and servicing Ecolab's accounts, and soliciting new business accounts through resources provided by Ecolab. *See id.* at ¶ 7.

C. Defendant Grailer's Employment Agreement

As a condition of Grailer's employment with Nalco/Ecolab she entered into an Employee Sales, Service, Marketing & Inventions Agreement (the "Grailer Agreement") (the Grailer

Agreement is attached hereto as **Exhibit B**). The Grailer Agreement contains among other things: (1) a non-disclosure of confidential information provision; (2) a return of property provision, and (3) non-deletion and non-transfer of data provisions. (Ex. B.)

Grailer's Agreement specifically restricts Grailer's retention, dissemination, and use of Ecolab's confidential information during and after separation of her employment. Defendant agreed "that while employed with the Company and for a period of three (3) years after termination of Employee's employment with Company" that she would hold such information "in a fiduciary capacity for the benefit of Company" and would not "directly or indirectly, use or disclose" any such information "that Employee may have acquired (whether or not developed or compiled by Employee and whether or not Employee was authorized to have access to such Confidential Information) during the term of, in the course of, or as a result of Employee's employment by Company." See **Exhibit B**, ¶ 2.

The Employee Agreement defined Confidential Information as:

Company's confidential data or information which is valuable to Company but substantially inaccessible to the public and to competitors of Company, including, without limitation, business information, financial data, product information, the identities and contact information of actual or potential customers or suppliers, pricing information, and other information of a proprietary nature regarding the Company's business operations, excluding Trade Secrets. Notwithstanding the foregoing, the term "Confidential Information" shall not include information that Employee can establish by competent proof: (i) was generally known to or accessible by the public at the time Company disclosed the information to Employee; (ii) became generally known to or accessible by the public after disclosure by Company through no act or omission by Employee; or (iii) was disclosed to Employee, after the Employee's termination of employment with the Company, by a third party having a bona fide right both to possess the information and to disclose the information to Employee, provided such third party is not subject to an obligation of confidentiality with respect to such information.

See **Exhibit B**, ¶ 2.

Defendant's Employment Agreement further requires her to return Nalco/Ecolab its property and information upon separation, to not transfer company data to unapproved devices, and upon considering leaving her employment with Plaintiffs to not transfer or erase any Company information as follows:

Maintain Confidentiality

"Employee agrees that while employed with the Company and for a period of three (3) years after termination of Employee's employment with Company, Employee will hold in a fiduciary capacity for the benefit of Company and shall not, directly or indirectly, use or disclose any Confidential Information, as defined hereinafter, that Employee may have acquired (whether or not developed or compiled by Employee and whether or not Employee was authorized to have access to such Confidential Information) during the term of, in the ... "

(Exh. B, ¶ 2.)

Return of Company Property

"Upon termination of Employee's employment and/or promptly upon request, the Employee will return in good order all Company property and information in the Employee's possession, custody or control. Upon termination, Employee shall return all Company data, business information, credit cards, keys, automobile, and any other Company property in his possession. Employee shall not erase or delete any Company data from Company phones or computer or other electronic devices except as may be necessary in the regular course of conducting business for the Company. For example, it would be a violation of this provision for Employee to accept a position with another entity and/or give notice of Employee's resignation and then delete and/or erase Company data from Employee's Company assigned phone and/or computer device."

(Exh. B, ¶ 11.)

Not Transfer Company Data to Unapproved Devices

"Employee agrees that Employee will not transfer or store any Company information on any device or other storage medium (physical or virtual) not provided or authorized by the Company unless authorized to do so in writing by the Company."

Upon considering leaving the Company to not transfer or delete company information.

“As soon as Employee begins to consider leaving the Company or Employee realizes Employee’s employment with the Company has or will soon come to an end, Employee will not wipe, delete or transfer or cause any Company data to be wiped, deleted or transferred from any such device before returning the device to the Company.”

(Exh. B, ¶ 4.)

D. Grailer’s Voluntary Resignation and Theft of Ecolab’s Confidential and Trade Secret Information

On January 8, 2023, Grailer informed her supervisor, Joshua Galliard, that she was voluntarily resigning to join a competitor. *See Exhibit A ¶ 10.* Mr. Galliard instructed her that she was immediately relieved of all of her duties and expressly told her not to “steal” the company’s confidential information. *See Exhibit A ¶ 10.*

On January 11, 2023, Grailer returned her Ecolab issued laptop computer. *See Exhibit A ¶ 11.*

Plaintiffs’ IT department was thereafter alerted that Grailer on January 15, 2023 had accessed Ecolab’s cloud-based network and accessed numerous confidential documents. *See Exhibit A ¶ 12-14.* Grailer had no reason to access the documents at that time as she was no longer employed by Nalco/Ecolab and moreover many of the documents misappropriated had no relation to her prior duties at Nalco. *See Exhibit A ¶ 16.*

The Company then retained a computer forensic expert to uncover the full extent of Defendant’s misappropriation. The Company’s forensic examiner’s investigation confirmed that on January 15, 2023, several days after her separation from employment, Defendant unlawfully accessed the Company’s computer network through the cloud and accessed 20 files containing highly confidential and trade secret information concerning the Company’s business and customers. *See Exhibit C ¶ 16-17.*

The forensic investigation further revealed that Defendant Grailer accepted employment with ChemTreat, a direct competitor of Plaintiffs in the water treatment industry, on December 21, 2022. (**Exhibit C**, Lieb Declaration at ¶ 18.) However, it was not until January 8, 2023 that she gave notice of her resignation and proceeded to access and download hundreds of company documents containing company confidential and trade secret information. Grailer had no legitimate business reason to access these files.

Specifically, the forensic examiner's investigation revealed that on January 8, 2023 at 9:39 p.m., Defendant Grailer attached an external USB drive to her company-issued laptop. Forensic analysis of the company-issued computer revealed Grailer exfiltrated 159 files on January 8, 2023 at 7:20 p.m. and 2 files at 8:48 p.m. *See Exhibit C* ¶ 30. The analysis further revealed that Grailer exfiltrated one PDF document on January 8, 2023 at 8:56 p.m., 128 Excel documents on January 8, 2023 at 7:33 p.m. and 9:04 p.m. *See Exhibit C* ¶ 32. Finally, the analysis revealed that Grailer exfiltrated 43 pictures on January 8, 2023 at 9:11 p.m. *See Exhibit C* ¶ 33.

The documents exfiltrated by Ms. Grailer on January 8, 2023 contained highly confidential information of Ecolab including without limitation confidential information such as detailed customer service reports, sales quotes, key performance indicators for customers, detailed pricing information, field service pricing, wastewater trial calculations, return on investment information, chemical formulations, detailed product information, proprietary information regarding developing technology such as Evaporation Treatment Technology, boiler calculations, customer specific processes and calculations, dosage calculations, and Nalco's proprietary Light N.A. Pricing tool. (**Exhibit A** ¶ 17; see also **Exhibit C**.)

The Company's forensic examination has further revealed that Defendant Grailer also improperly deleted Company data from her company assigned phones which is a blatant breach of

her Employment Agreement. Defendant Grailer attached her company-issued iPhone 6S to her company-issued laptop and factory reset the phone before returning it to Nalco/Ecolab. (**Exhibit C** ¶ 16.) Defendant Grailer also changed the AppleID email address associated with the iPhone 6S from jlgailer@ecolab.com to a non-Ecolab email address. (Exh. C, ¶ 23.) This prevented Nalco/Ecolab from accessing the Apple iCloud account associated with the iPhone 6S. This was expressly prohibited by Defendant Grailer’s Employee Agreement. **Exhibit B** ¶ 4.

On January 31, 2023, Nalco/Ecolab, through undersigned counsel, sent Grailer a letter via Federal Express notifying Grailer that Nalco/Ecolab was aware she had accessed and downloaded numerous files containing Ecolab’s confidential and trade secret business information. *See Exhibit D*. In the letter, Ecolab requested that Grailer preserve the misappropriated files and contact undersigned counsel immediately to arrange for the return of Ecolab’s data. To date, Grailer has not contacted undersigned counsel.

III. LEGAL STANDARD

A court may grant a temporary restraining order or a preliminary injunction when a plaintiff demonstrates the following elements: (1) a substantial likelihood of success on the merits; (2) an irreparable injury will occur absent issuance of the injunction; (3) the injunction would not substantially harm the non-moving parties; and (4) the injunction, if issued, would not be adverse to the public interest. *Christian Legal Soc’y v. Walker*, 453 F.3d 853, 859 (7th Cir. 2006). A temporary restraining order and a preliminary injunction “are designed to protect against irreparable injury and preserve the court’s power to render a meaningful decision after a trial on the merits.” *Democratic National Committee v. Bostelmann*, 447 F.Supp.3d 757, 764 (W.D.WI. 2020). “It is within the discretion of the Court to grant a motion for preliminary injunctive relief

when the moving party satisfies its burden of persuasion as to each” of the prerequisites. *Ohio-Sealy Mattress Mfg. Co. v. Duncan*, 486 F.Supp. 1047, 1052 (N.D.Ill. 1980).

IV. ARGUMENT

In order to obtain a temporary restraining order and/or preliminary injunction, Plaintiffs must establish that: (1) it has a likelihood of prevailing on the merits of its claim; (2) it will suffer irreparable injury if the relief is not granted; (3) the threatened injury to Plaintiffs outweighs the harm the relief would inflict on Grailer; and (4) if granted, the injunction would not be adverse to the public interest. Plaintiffs are entitled to preliminary injunctive relief because they can establish each of these factors.

a) Plaintiffs Likely to Succeed on the Merits of Their Claims

1) Plaintiffs Are Likely if Not Certain to Succeed on their Defend Trade Secrets Act and Wisconsin Trade Secrets Act Claims

To plead a violation of the DTSA and Wisconsin’s Uniform Trade Secret Act (“UTSA”), a plaintiff must allege that it “(1) the defendant acquired, used, or disclosed the information through improper means; and (2) the information at issue qualifies as a trade secret.” *DF Institute, LLC v. Dalton Edu., LLC*, 2020 WL 4597122, at *2 (W.D.Wisc. Aug. 11, 2020) (citing 18 U.S.C. § 1689(5); Wis. Stat. § 134.90(2)). Specifically, to establish a claim for misappropriation of a trade secrete under the UTSA, a plaintiff must show: (1) the information is economically valuable; (2) the value is the result of not being generally known to or readily ascertainable by others who could obtain value from it; (3) the plaintiff took reasonable steps to maintain its secrecy; and (4) the defendant misappropriated the information. *See Edgenet, Inc. v. GSI AISBL*, 742 F.Supp.2d 997 (E.D.Wisc. 2010).

Plaintiffs have alleged and identified those trade secrets that they took reasonable measures to keep those trade secrets secret, the trade secrets are not generally known or ascertainable through

proper means, the trade secrets have independent economic value, and Grailer has misappropriated the trade secrets by improper means.

A trade secret, under the DTSA, means “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices” 18 U.S.C. 1839(3). The UTSA definition of trade secret is nearly identical. A trade secret under the UTSA is defined as: “information, including a formula, pattern, compilation, program, device, method, technique or process to which all of the following apply: 1. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use. The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.” *Danaher Corp. v. Lean Focus, LLC*, 2021 WL 3190389, at *13 (W.D.Wisc. July 28, 2021) (quoting Wis. Stat. § 134.90(1)(c)) (internal quotation marks omitted).

Nalco/Ecolab makes great efforts to protect its trade secrets and confidential information. These efforts include: (1) restrictive covenant agreements with high level employees; (2) handbook and IT policies; (3) IT security measures, such as password protections for all computers and segregation of certain files so that only employees with a need to access can access certain confidential information. (Exh. A, ¶ 9.)

Here, Defendant Grailer accessed thousands of Company documents containing highly confidential and trade secret information including technical information, client data, developmental information. (Exh. C.) It is beyond reasonable dispute that Defendant Grailer misappropriated Ecolab’s trade secrets and confidential information.

2) Plaintiffs Are Highly Likely, if Not Certain, to Succeed on the Merits of its Computer Fraud and Abuse Act claim

The CFAA provides, “[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer. . . shall be punished as provided in subsection (c) of this section.” 18 U.S.C.A. § 1030(a)(2)(C). The Act provides that a person who accesses a computer with authorization, nevertheless “exceeds authorized access” if he uses his access “to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter.” 18 U.S.C.A. § 1030(e)(6).

Plaintiffs have suffered damage or loss based on a violation of the Act. 18 U.S.C.A. § 1030(g). A civil claim under the Act may be brought by any person who has suffered or would have suffered damages, loss or injury as described in Sections (a)(5)(B)(i)-(v) of the Act. A “loss” is defined in the Act as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C.A. § 1030(e)(11).

Defendant Grailer violated Section (a)(4) of the Act because she “knowingly and with intent to defraud” accessed Nalco/Ecolab’s computer files “without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud” and she obtained a thing of value. 18 U.S.C.A. § 1030(a)(4). Defendant Grailer’s wrongful access of Ecolab’s computer networks without authorization, at a time she was no longer employed with Ecolab, and after expressly being instructed that she was no longer authorized to access Ecolab’s computer devices or computer network, constitutes a blatant violation of the Computer Fraud and Abuse Act.

Plaintiffs have suffered and continue to suffer loss and damage to the integrity of their data, computer systems and loss of confidential information and trade secrets, resulting in damages far

in excess of \$5,000.00 and absent injunctive relief will continue to suffer irreparable harm and damages.

3) Plaintiffs Can Demonstrate They Are Highly Likely, if Not Certain to, Succeed on Their Breach of Contract Claims

Defendant Grailer entered into a valid and enforceable Employment Agreement with Ecolab which requires her to, among other things: maintain confidentiality, return company property, and not transfer company data to unapproved devices, and not delete company data when considering leaving the Company. Defendant Grailer has brazenly breached all of the aforementioned provisions:

- By retaining and failing to return Ecolab's property and information at the end of her employment with the company;
- by transferring company data to unapproved devices;
- by transferring company data after she had accepted employment with a competitor, and;
- by erasing data from her company assigned telephone.

Indeed, in this case, not only did Defendant Grailer fail to return the hundreds of documents she misappropriated but she also egregiously misappropriated the Company's confidential information without authorization after her separation by way of the iCloud.

b) Plaintiffs will suffer irreparable injury if the relief is not granted and the threatened injury to Plaintiffs outweighs the harm the relief would inflict on Grailer

The balance of harms weighs in favor of granting injunctive relief to Ecolab. Through years of research, financial and human capital investment, Ecolab has compiled and maintained confidential business information which provides it with a competitive advantage. Defendant Grailer unlawfully misappropriated confidential and trade secret information from Ecolab, including Ecolab's pricing, pricing histories, customer specific account information, customer

contact information, margins, chemical mix and chemical formulations. Ecolab's business will be compromised and irreparably harmed if its competitor is permitted to unfairly compete in the highly competitive water treatment industry armed with Plaintiff's confidential and trade secret information. Defendant Grailer, on the other hand is not harmed at all, she is only required to comply with her contractual obligations and compete fairly without the aid of Ecolab's confidential and trade secret information. Accordingly, the balance of harms weighs in favor of Nalco/Ecolab and the granting of injunctive relief.

c) If granted, the injunction would not be adverse to the public interest

Granting Plaintiffs' Motion will advance the public interest. The public interest favors enforcement of contracts and the protection of trade secret information gathered and developed by a company at significant expense. An injunction will protect plaintiff's and the public's interests in the protection of trade secrets but will not place an undue burden on fair competition. *La Calhene, Inc. v. Spolyar*, 938 F.Supp. 523, 531 (W.D.Wisc. 1996). Further, the public interest is embedded in the UTSA and DTSA both of which expressly provide for injunctions in cases of "actual or threatened misappropriation" of trade secrets such as that in this case. 18 U.S.C. 1836(b)(3)(a); Wis. Stat. § 134.90(2).

V. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court enter a temporary restraining order and preliminary injunction as follows:

- 1) Defendant, her agents, servants, employees, representatives, and attorneys, and other persons who are in active concert or participation with any of the foregoing (collectively, "Covered Persons") are restrained and enjoined as follows:
 - a. Directly or indirectly, disclosing or making any use of any Trade Secret and Confidential Information of Ecolab and Nalco;

- b. Provide a full and complete accounting of all electronic devices, email accounts, cloud-storage accounts, and other devices/accounts that Grailer had access to in the last year of her employment with Plaintiff and that Plaintiff's business information could have been downloaded and/or copied to;
- c. Take all necessary steps to maintain and preserve all potentially relevant evidence regarding the allegations in the Complaint, including, but not limited to, all indicia and potential evidence relating Grailer's misappropriation of Ecolab's trade secrets and confidential/proprietary information and her and others potential access of that same information by any and all electronic devices, email accounts, including internet e-mail accounts, cloud-storage based accounts, and the like within its possession, custody or control;
- d. Immediately make available for inspection and imaging all computers, external storage devices, mobile devices, and all personal Cloud and email accounts including internet-based e-mail accounts in Grailer's possession and/or control, to determine the full extent of Defendant Grailer's access, possession, retention, and use of Ecolab's confidential information or trade secrets;
- e. The Covered Persons return to Plaintiffs any Trade Secret and Confidential Information that is in their possession, custody, or control (including but not limited to Trade Secret and Confidential Information in paper form and in electronic form, wherever and however stored, including but not limited to personal computers, cloud storage, external storage media, smart phones and other handheld devices, and email accounts) and to the extent that any such information is maintained in electronic form;
- f. Until further Order of the Court, the Covered Persons are restrained from conducting, carrying on, or engaging in any competitive business that was developed and/or implemented, in whole or in part, directly or indirectly, through the use of any Company Trade Secret and Confidential Information, (the "Prohibited Business"); and
- g. That the Court should schedule a preliminary injunction hearing and then issue a preliminary injunction on the terms set forth herein, as well as including any additional relief that may be warranted.

Dated this the 23rd day of February, 2023.

Respectfully submitted,

ECOLAB INC.,
By Counsel

/s/ Craig R. Annunziata

Craig R. Annunziata
Daniel F. Lanciloti (*admitted Pro Hac Vice*)
James M. Hux, Jr. (*admitted Pro Hac Vice*)
FISHER PHILLIPS LLP
10 South Wacker Drive
Suite 3450
Chicago, Illinois 60606
Telephone: (312) 346-8061
Facsimile: (312) 346-3179
cannunziata@fisherphillips.com
dlanciloti@fisherphillips.com
jhux@fisherphillips.com

ATTORNEY FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that on the 23rd day of February 2023, the foregoing document was electronically filed with the Clerk of Court using the CM/ECF system and was served on the following by FedEx to the Plaintiff:

Jessica Grailer
1926 Hawks Ridge Drive, #308
Verona, WI 53593

Respectfully submitted,

/s/ Craig R. Annunziata